UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/933,972	08/20/2001	Philip Hawkes	010497	7964

23696 7590 11/19/2007
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

NOTIFICATION DATE	DELIVERY MODE
11/19/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/933,972
Filing Date: August 20, 2001
Appellant(s): HAWKES ET AL.

Won Tae C. Kim, Reg. No. 40,457
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/29/2007 appealing from the Office action mailed 8/3/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,690,795	RICHARDS	2-2004
6,073,122	WOOL	6-2000

LinuxGuruz. "FOLDOC, Free On-Line Dictionary of Computing", 12/19/2000.

Schneier, Bruce. Applied Cryptography, Second Edition, 1996 John Wiley & Sons, Inc., pp. 182-184.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-5, 10-11, 13-16 & 18-24 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,690,795 to **Richards**.

Regarding claims 1-5, 11, 13-14 & 22-24, Richards discloses determining a registration key (UEV) specific to a participant (set top box) in a transmission (Fig. 26, #130 & col. 20, lines 61-67), determining a first key (CCK_1, Fig. 26, #133), encrypting the first key (CCK_1) with the registration key (Fig. 26, #133), sending the encrypted first key ([CCK_1]UEV) to the participant in the transmission (set top box, Fig. 26, #133), determining a second key (PK and SK) for decrypting content on a broadcast channel (Fig. 26, #159), encrypting the second key with the first key ([PK]CCK_1, [SK]PK) updating the first key (CCK) after a first time period has elapsed (Fig. 23) and updating the second key (SK and PK) after a second time period has elapsed, wherein the second key is updated in two parts (SK and PK), the first part (PK) known to the participant in the transmission (PK must be known to decrypt SK, Fig. 26 & col. 13, lines 47-49) and a second part (SK) send on the broadcast channel (Fig. 26).

Regarding claim 10, Richards discloses transmitting the encrypted first key (PK) and transmitting the encrypted second key (SK, col. 9, line 58 – col. 10, line 5).

Regarding claims 15 & 16, Richards discloses in a wireless system (col. 20, lines 61-67) determining a registration key (UEV) specific to a participant (set top box) in a transmission

(Fig. 26, #130), determining a first key (CCK_1, Fig. 26, #133), encrypting the first key (CCK_1) with the registration key (Fig. 26, #133), sending the encrypted first key ([CCK_1]UEV) to the participant in the transmission (set top box, Fig. 26, #133), determining a second key (PK and SK), encrypting the second key with the first key ([PK]CCK_1, [SK]PK) updating the first key (CCK) after a first time period has elapsed (Fig. 23) and updating the second key (SK and PK) after a second time period has elapsed, wherein the second key is updated in two parts (SK and PK), the first part (PK) known to the participant in the transaction and a second part (SK) sent on a broadcast channel (Fig. 26), a user identification unit (set-top box, col. 4, lines 55-62), operative to recover a short-time key (SK) for decrypting a broadcast message (content, col. 9, lines 11-33), comprising a processing unit (decryption hardware) to decrypt key information (col. 9, lines 11-33) and a mobile equipment unit (decryption hardware) adapted to apply the short-time key for decrypting the broadcast message (content, col. 4, lines 55-62 & col. 9, lines 11-33).

Regarding claim 18, Richards discloses the memory storage unit storing a broadcast access key (PK) and wherein the processing unit decrypts the short-time key (SK) using the broadcast access key (PK, col. 5, lines 45-64 & col. 9, lines 56-63).

Regarding claim 19, Richards discloses the short-time key (SK) being updated at a first frequency (col. 9, lines 32-36 & Fig. 16).

Regarding claim 20, Richards discloses the broadcast access key (PK) being updated at a second frequency less than the first frequency (Figs. 9 & 10).

Regarding claim 21, Richards discloses a video service (col. 2, lines 39-55).

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards**, as applied to claim 4 above, in further view of "FOLDOC, Free On-Line Dictionary Of Computing" by **LinuxGuruz**. Richards discloses using the system for distributing information on computer networks, but lacks specifically Internet Protocol packets. However, LinuxGuruz teaches that Internet Protocol packets are widely used on Ethernet networks for packet routing (§Internet Protocol). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to broadcast Internet Protocol packets. One of ordinary skill in the art would have been motivated to perform such a modification because Internet Protocol packets are used on Ethernet networks, as taught by LinuxGuruz (§Internet Protocol).

Claims 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards**, as applied to claim 3 above, in further view of Applied Cryptography, Second Edition by **Schneier**.

Regarding claim 7, Richards lacks calculating a registration key information message and transmitting the registration key information message. However, Schneier teaches that no encryption key should be used for an indefinite period (p. 183, §8.10) and should be replaced (p. 184, ¶3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to update the registration key and hence calculate a registration key information message and transmit the registration key information message. One of ordinary skill in the art would have been motivated to perform such a modification to update the registration key, as taught by Schneier (pp. 183-184).

Regarding claim 8, Richards discloses calculating a first key (PK) information message (new encrypted key) and transmitting the first key information message (col. 10, lines 1-5).

Regarding claim 9, Richards discloses calculating a second key (PK) information message (new encrypted key) and transmitting the second key information message (col. 9, lines 58-62).

Claims 12 & 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards**, as applied to claims 11 & 15 above, in further view of U.S. Patent 6,073,122 to **Wool**. Richards discloses storing the second key (SK) in a memory storage unit (col. 5, lines 60-63), but lacks the first key stored in secure memory storage unit. However, Wool teaches that set-top boxes often contain secure memory to minimize piracy of encryption keys stored (col. 1, lines 44-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store the first key in a secure memory storage unit. One of ordinary skill in the art would have been motivated to perform such a modification to minimize piracy of encryption keys stored, as taught by Wool (col. 1, lines 44-52).

(10) Response to Argument

Appellant's brief (§7A)

Appellant's brief (p. 13, ¶1) argues that Richards does not disclose "a second key for decrypting content on a broadcast channel" because Appellant's first key is equated to Richards' "CCK_1" and Appellant's second key is equated to Richards' keys "PK and SK" and the "encrypting the second key with the first key" is equated with Richards' "[PK]CCK_1,[SK]PK". As such, Appellant alleges that the "second key", equated by the examiner to "PK and SK" are

not both encrypted by the alleged "first key", i.e. CCK_1. However, as Appellant states, Richards disclosure of, for example, [PK]CCK_1 is read as PK, encrypted by CCK_1.

{*Brief explanation of Richards*} Richards' Fig. 26 discloses the general concept of Richards, where CCK_1, encrypted by UEV is provided to the set top box, and the set top box uses UEV (something it already has) to decrypt [CCK_1]UEV to recover CCK_1 (#133). CCK_1 is then used to decrypt a copy of itself (#138), which is not pertinent to the present rejection. In step 144, the previously-recovered CCK_1 is used to decrypt the package [PK]CCK_1 to recover PK. In step 152, the previously-recovered PK is used to decrypt the package [SK]PK to recover SK. In step 165, the previously-recovered SK is used to decrypt the package [CONTENT]SK to recover CONTENT.

Appellant argues that PK and SK are not both encrypted by CCK_1. However, CCK_1 is required to recover PK, which is required to recover SK (col. 9, lines 26-28). Without CCK_1, the value of SK would remain scrambled. CCK_1 directly encrypting PK and PK encrypting SK represents CCK_1 encrypting PK and SK, but the mathematical process takes multiple steps. Therefore, it is submitted that these steps (144 and 153) represent a decryption of PK and SK using CCK_1. The broad language used to define the claim does not require a specific algorithm or mathematical function to be performed in the step of the first key encrypting the second key. Further, this decryption shown in Fig. 26 is the 'un-doing' of the encryption of these keys (also see col. 11, lines 45-51, which discloses the keys that are encrypted, col. 13, lines 47-49, which explains that CCK is required to gain access to SK and PK & col. 11, lines 53-55, which describes that the encryption processes, i.e. cable provider, provides [PK]CCK and [SK]PK for each CCK). It is further noted that Appellant's invention combines two data values to create the

"second key" (specification, ¶1069), however, claims recite broad language that does not include this feature.

Appellant's brief (p. 13, ¶2 – p. 14, ¶1) argues that the claimed "second key" cannot be equated to Richards' "SK and PK" because SK and PK are two values. However, further in the claim it is seen that Appellant is in fact claiming that the second key is represented by two, separately-updatable, parts. Further, Fig. 20 & accompanying disclose col. 12, lines 18-20 shows that at some points, both SK and PK are updated. Therefore, this argument is contradictory. Further, Appellant argues that "SK and PK" does not decrypt content, as claimed. However, similarly to the previous response, it is the Examiner's submission that because the CONTENT is directly decrypted using SK, which must be itself decrypted using PK, than the key "SK and PK" is encrypting the content. Without PK, the content could not be decrypted (see Fig. 26, #152 and #159). The claims do not recite that the entirety of the second key be mathematically combined with the encrypted content in any particular algorithm, only that the second key (a data value) be used to decrypt the content. In fact, for example claim 1 recites "second key for decrypting content …". It is submitted that SK and PK are both used, in sequence, "for decrypting content" (see sequence of Fig. 26).

Appellant's brief (p. 14, ¶2) argues that the claimed second key updated in two parts cannot be equated to PK and SK, each updated (the updating of PK and SK is shown on, for example, Fig. 23, where the dots represent a key update/replacement and the numbers at the top of the grid represent the movement of time). As such, the claimed second key, i.e. Richards' SK and PK is updated in two parts, PK being known to the participant (PK is known before SK is accessed) and the second part (SK) sent on the broadcast channel. As seen in Fig. 23 and also in

col. 9, lines 46-52, as time passes, each part of the "second key" is change via changing SK and PK. Therefore, as stated, it is submitted that the Examiner's position that PK and SK can reasonably be interpreted as the claimed second key. It is noted that in embodiments of Appellant's invention, part of the second key is a static value that is read from the device. However, limitation is also not claimed.

Appellant's brief (§§7A-7D)

Appellant's brief (pp. 15-16) argues that the dependent claims are allowable over the art for the same reason as previously argued with respect to the independent claims. Therefore, the Examiner submits that the response as recited above is sufficient to show that the rejections are reasonable..

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Michael J. Simitoski/

Conferees:

Kim Vu

SUPERVISORY PATENT
TECHNOLOGY CENTER

Kambiz Zand

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER